Commonwealth Fusion Center
Standard Operating Procedure

Effective Date	Number
August 30, 2011	CFC-02

Subject:

Commonwealth Fusion Center Privacy Policy

PURPOSE

The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are collected, analyzed, developed and exchanged pertaining to suspicious activity reporting and the Information Sharing Environment. Furthermore, this privacy policy assists its authorized users in:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.
- Preventing and disrupting potential terrorist attacks.
- Protecting individual privacy, civil rights, civil liberties, and other protected interests.
- Minimizing the threat and risk of damage to real or personal property.
- Protecting the integrity of the criminal investigatory process, criminal intelligence, and justice system processes and information.
- Minimizing reluctance of individuals or groups to use or cooperate with the justice system.

COMPLIANCE WITH LAWS REGARDING PRIVACY, CIVIL RIGHTS AND CIVIL LIBERTIES

All CFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the center's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment (ISE)participating centers and agencies), and participating

justice and public safety agencies, as well as to private contractors, private entities, and the general public.

All CFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable state and federal law protecting privacy, civil rights, and civil liberties, including, but not limited to, the constitutions of the United States and the Commonwealth of Massachusetts, and the following:

- MGL c. 22C, § 38 (Criminal Information).
- MGL Chapter 4, §7, cl. 26 (a)-(s) (Public Record Exemptions).
- 28CFR Part 23 related to Criminal Intelligence Systems.
- MGL c. 6, § 167 *et seq.* (Criminal offender Record Information).
- MGL c. 66, §10 (Public Records Law).
- MGL c. 66A, §1 (Fair Information Practices).
- MGL c. 272, §99 (Wiretap Law);
- MGL c. 41, §98F (Daily Logs);
- MGL c. 41, §97D (Rape and Sexual Assault Reports).
- MGL c. 265, §24C (Confidentiality of Alleged Rape Victim's name);
- MGL c. 93H, §1 *et seq.* (Security Breach/Personal Information)
- 18 USC 2722 (Federal Driver's Privacy Protection Act).
- Laws and statutes applicable to victim rights and confidentiality
- Laws applicable to juvenile confidentiality.

The CFC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the listing of applicable state and federal privacy, civil rights, and civil liberties laws listed above.

GOVERNANCE AND OVERSIGHT

The Massachusetts Department of State Police ("MSP") oversees CFC operations. A MSP Commander supervises the overall operations of the CFC.

The MSP shall designate a Department staff member to serve as the Privacy Officer for the Center and will be trained in Privacy and Civil Rights and Civil Liberty issues. The Privacy Officer is the point of contact for reporting alleged errors and violations of the center's privacy policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: Office of the Chief Legal Counsel, Massachusetts State Police General Headquarters, 470 Worcester Rd., Framingham, MA 01702 ATTN: CFC Privacy Officer.

The MSP Commander is responsible for the implementation of the privacy policy.

There shall be a Privacy Oversight Committee that shall advise the MSP Commander upon his request and make recommendations to the MSP Commander to assist the CFC in ensuring that privacy and civil rights are protected as provided in this policy and by the center's information-gathering and collection, retention, and dissemination processes and procedures. The committee will annually review and recommend updates to the policy to the MSP Commander in response to changes in law and implementation experience.

The MSP Commander ensures enforcement procedures and sanctions as outlined in this policy are adequate and duly enforced.

The MSP Commander or his/her designee shall liaise with the community to ensure that privacy and civil rights are protected as provided in this policy.

The MSP Commander, and/or CFC administrator(s) designated by the MSP Commander, shall establish access guidelines and shall record the access authority level of all CFC personnel.

The MSP Commander and/or CFC administrator(s) designated by the MSP Commander shall maintain CFC information including access to, adding of, and/or printing of, CFC information. Access to the CFC information will be granted only to center personnel whose position and job duties required such access; who have successfully completed a background check and appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly.

An audit trail shall be maintained relative to access history and disclosure of CFC information.

DEFINITIONS

Primary Terms and definitions used in the CFC are located in Appendix A.

CFC INFORMATION

The CFC serves as the central law enforcement operating facility within the Commonwealth of Massachusetts, whose primary purpose relates to the receipt, retention, evaluation, and dissemination of information concerning criminal activity, including terrorist activity.

The CFC works with various federal, state, and local law enforcement agencies, including non-law enforcement groups such as the public health department, fire departments, campus police agencies, and the private sector.

The CFC will only seek or retain information that:

- Is reasonably based on a possible threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) activity that presents a threat to any individual, the community, or the nation and that the information is

relevant to the criminal (including terrorist) conduct or activity, or

- Is relevant to the investigation of suspected criminal (including terrorist) activities; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
- Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); or
- Is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

The CFC will not seek or retain, and information originating agencies will agree not to submit, information about individual(s) or organization(s) solely on the basis of their political, religious, or social views or activities; their participation in a non criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

CFC personnel, upon receipt of information, shall assess and review the information to determine its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

CFC personnel shall apply, to the maximum extent feasible, labels to agency-originated information or ensure that the originating agency has applied labels, if applicable, to indicate to the accessing authorized user that:

- The information is subject to state or federal law, as identified in this policy, restricting access, use, or disclosure.
- The information is protected information to include personal information on any individual (See Appendix A, Definitions) and, to the extent

expressly provided in this policy, includes organizational entities.

The CFC shall keep a record of the source(s) of all information sought and collected by the center.

CFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. CFC Personnel, prior to allowing access to, or dissemination of, CFC information, shall ensure that:

- Reasonable attempts to validate or refute the subject information have taken place.
- The information has been analyzed for sensitivity and confidence.
- Reasonable attempts to evaluate or screen the information have been made in order to assess the information's credibility and/or reliability.
- Any information whose credibility and/or reliability is invalidated, or otherwise unsubstantiated, is categorized as uncorroborated or unreliable as the case may be.
- Standardized reporting formats and data collection codes are utilized for SAR information.
- The information is retained or stored by using the same storage system used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to distinguish it from other information.
- Access to, or dissemination of, the information uses the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination).
- Regular access to CFC information is provided in response to an interagency inquiry by a law enforcement, homeland security, or public safety agency, for analytical purposes, or in the event that access to information by any public safety agency, entity, individual, or the public is required to respond to a situation involving serious and imminent danger to life or property.
- Timely and immediate steps are taken within one (1) year or less of receipt of information (a) to validate any otherwise un-validated tip, lead, or SAR information to determine its credibility or law enforcement value, and (b) to assign a

"disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) such that a subsequently authorized user is aware of the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

- The center's physical, administrative, and technical security measures are adhered to in order to ensure the protection and security of tips, leads, and SAR information.

The CFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

The CFC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to, metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

ACQUIRING AND RETAINING INFORMATION

Information gathering (acquisition and access) and investigative techniques used by the CFC and originating agencies will comply with all applicable laws and regulations, including, but not limited to:

- 28 CFR Part 23 regarding criminal intelligence information.
- The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- Constitutional provisions; applicable Massachusetts code provisions and administrative rules (including those cited in the "Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties" section of this policy), as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

The CFC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. CFC

personnel will be trained to recognize behaviors and incidents that are indicative of criminal activity related to terrorism. To the extent feasible, the CFC will train outside law enforcement members to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

The CFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities determined to be consistent with criminal activities associated with terrorist activity will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

Information gathering and investigative techniques used by the CFC will, and those used by originating agencies, be the least intrusive means necessary in the particular circumstances to gather information it is legally authorized to seek or retain.

The CFC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information are in compliance with applicable law and that these methods are not based on misleading collection practices.

External agencies that access the CFC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

The CFC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
- An individual who or information provider that is legally prohibited from obtaining or disclosing the information, except as otherwise authorized by law.

CLASSIFICATION OF INFORMATION

At the time of retention in the CFC system, information received by the CFC will be reviewed and labeled to reflect the information's source, validity, and reliability. This review, to the maximum extent possible, shall include an evaluation of:

- The veracity of the source (for example, anonymous tips, trained interviewer or investigator, public record, private sector);
- The validity of the content (for example, verified, partially verified, unverified, or unable to verify); and

- The reliability of the source (for example, completely reliable, usually reliable, unreliable, reliability unknown).

The labeling and classification of retained or existing information will be reevaluated by the CFC whenever new information is received or added. The purpose of the evaluation will be to determine what impact or effect, if any, additional information has on the reliability and/or veracity of previously received and/or retained information and to reclassify information accordingly.

The CFC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

The labeling and/or classification of retained or existing information will be reevaluated by the CFC whenever new information is added that has an impact on access limitations or the sensitivity of disclosure of the information.

At the time a decision is made by the CFC to retain information, CFC personnel shall label the information in accordance with this policy (by record, data set or system of records), and shall take all necessary steps, to the maximum extent feasible and pursuant to applicable limitations on access and disclosure, to:

- Protect confidential sources and law enforcement undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy or his or her civil rights and civil liberties.
- Ensure that confidentiality restrictions based on the individual's status (i.e. as a child, sexual abuse victim, or resident of a domestic abuse shelter, etc.) are complied with in accordance with applicable law.

The access classifications established under applicable guidelines shall determine the user's access authority level. The access authority level controls the range and scope of information to which authorized CFC personnel have access and what information authorized CFC personnel can add, change, remove, or print. The access authority level shall determine to whom CFC information can be disclosed and under what circumstances.

The CFC shall ensure that basic descriptive information labels are entered and electronically associated with data which is subject to confidentiality laws, rules, or policies pertaining to access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include, but are not limited to, the following:

- The name of the originating center, department or agency, component, and subcomponent.
- The name of the center's justice information system from which the information is disseminated.
- The date the information was collected.
- The title and contact information of the person to who questions regarding the information should be directed.

INFORMATION QUALITY ASSURANCE

The CFC will make reasonable efforts to ensure that information sought or retained is derived from dependable and trustworthy sources of information, accurate, relevant, complete, including the relevant context in which it was sought or received and other related information, and merged with other information about the same individual or organization only when the applicable criteria in "merging of information" section is met.

At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, compete, current, verifiable, and reliable).

The CFC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

The CFC shall conduct periodic data quality reviews of information it originates and shall make reasonable efforts to ensure that the existing information will be updated, corrected and/or removed from the system, or not used when the center determines that existing information is erroneous, misleading, obsolete, or otherwise unreliable, or in the event that the center determines that it did not have authority to collect the information or to provide it to another agency.

Originating agencies external to the CFC are responsible for reviewing the quality and accuracy of the data provided to the CFC. The center will review the quality of information it has received from an originating agency and will, in the event that the information received is suspect, inaccurate, incomplete, inaccurate, or otherwise unreliable or unsubstantiated, notify, in writing or electronically, the appropriate contact person in the originating agency.

The CFC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and will make reasonable efforts to correct, remove, or refrain from utilizing protected information which is determined to be erroneous or deficient.

In the event that the CFC determines that information previously provided to a recipient agency is deficient, the CFC will notify the recipient agency, in writing or electronically, and advise that the information which it previously provided to them is subject to removal or correction by the CFC as the information was determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

COLLATION AND ANALYSIS OF INFORMATION

Information sought or received by the CFC will only be analyzed by qualified individuals who have successfully passed a background check and have been properly trained to provide tactical and/or strategic intelligence pertaining to the existence, identification, and capability of individuals and organizations suspected of having engaged in, are engaging in, or intend to engage in criminal activities, including terrorist activities.

Information acquired or received by the CFC, identified in "CFC Information" or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to further crime and terrorism prevention, enforcement, force deployment, or prosecution objectives and priorities established by the agency.

Information sought or received by the CFC or from other sources will not be analyzed or combined in an unlawful manner or for an unlawful purpose.

The CFC requires that all appropriate analytical products, as determined by CFC Commander, be reviewed and approved by the CFC Commander or the Commander's designee to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

MERGING OF INFORMATION

Information pertaining to an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information pertains to the same individual or organization.

In determining whether information pertains to a specific identified individual or organization sufficient to permit merger, the CFC shall utilize reasonable steps to identify the subject individual. The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and/or organization and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, marks or scars; social security number;

driver's license number; other biometrics such as DNA, retinal scan, or facial recognition.

Such efforts may also include or entail a review of identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the organization's name, federal or state tax ID number, address information and telephone number.

If matching requirements are not fully met but there is a strong partial match, the information may be associated if accompanied by a clear statement that is has not been adequately established that the information relates to the same individual or organization.

SHARING AND DISCLOSURE OF INFORMATION

Credentialed, role based access criteria will be used, as appropriate, to control:

- information to which a particular group or class of users can access based upon the group or class;
- the information a class of users can add, change, remove, or print; and
- to whom, individually, the information can be disclosed and under what circumstances.

Access to information which the CFC retains will only be provided to authorized CFC personnel or other authorized governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, and/or public health purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. Records retained by the CFC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

The CFC adheres to the current national standards including the current version of the ISE-SAR Functional Standard relative to the processing of suspicious activity reporting (SAR), including the use of a standard reporting format and commonly accepted data collection codes. The CFC utilizes a sharing process which complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

Agencies external to the CFC may not disseminate CFC information received from the CFC without prior approval from the originator of the information.

An audit trail will be kept of the identity of all persons who have accessed CFC information or to whom CFC information has been provided and will be sufficient to

allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.

Information gathered or collected and records retained by the CFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of two years by the center.

Nothing in this policy prohibits the dissemination of intelligence information to an otherwise authorized government official or to any other individual when necessary to avoid imminent or certain danger to life or property.

The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

DISCLOSURE OF INFORMATION TO PUBLIC (Redress)

Information gathered and retained by the CFC may be disclosed to a member of the public only in the event that the requested information is a public record as defined by G.L. c. 66, §10, or is not otherwise exempt from public disclosure by statute or law.

Subject only to the mandates of the CFC to comply with the Massachusetts Public Records Law or other applicable laws, the CFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself, unless otherwise required by law.

In the event that a member of the public submits a request under G.L. c. 66, §10, the Massachusetts Public Records Law, the CFC reserves the right to assert any exemption contained in G.L. c. 4, §7, cl. 26 (a) - (s) or assert any Massachusetts statute or law prohibiting the public disclosure of requested CFC documents.

Categories of records which are ordinarily exempt from public inspection and/or not otherwise subject to public disclosure include, but are not limited to, the following records:

- Records which are, expressly or by implication, statutorily confidential or not subject to public disclosure. See G. L. c. 4, §7, cl. 26 (a).
- Records that relate to any ongoing investigation or prosecution. See G.L. c. 4, §7, cl. 26 (f).
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section

606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010. See also, G.L. c. 66, §10.

- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under G.L. c. 4, §7, cl. 26 (f).
- Records relating to the physical safety of any individual. See G.L. c. 4, §7, cl. 26 (n)
- Records that would reveal scientific and technological secrets or the security plans of military and law enforcement agencies, the disclosure of which would endanger the public welfare and security. G.L. c. 4, §7, cl. 26 (a), (f), (n);
- Disclosure would constitute an unwarranted invasion of personal privacy. G.L. c. 4, §7, cl. 26 (c).
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, including vulnerability assessments, risk planning documents, needs assessments, and threat assessments. See G.L. c. 4, §7, cl. 26 (f) and (n).
- The information is in a criminal intelligence system subject to 28 CFR Part 23 or is otherwise required to be kept confidential by federal law or regulation or state law or rule of court. See G.L. c. 66, §10, G.L. c. 4, §7, cl. 26 (f).
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under the Access to Public Records Act, MGL, be shared without permission.

The CFC shall maintain an audit trail of all public inquiries received requesting CFC documents and, to the extent any information is furnished, shall include a description of any information disclosed in response to any public records request.

The CFC reserves the right to charge a fee for costs associated with researching or otherwise responding to a public records request in accordance with G.L. c. 66, §10 and 950 CMR 32.06.

Upon satisfactory verification of identity, any individual ("data subject") may access and review any personal data, as defined by G.L. c. 66A, §1 *et seq.* relating to the data

subject and which personal data is within the possession of the CFC. In accordance with G.L. c. 66A, §1 *et seq.*, and to the extent that the CFC possesses personal data, the data subject may access his or her personnel data for the purposes of challenging or contesting the accuracy or completeness of the information in accordance with G.L. c. 66A, §1 *et seq.* The CFC's response to the request for information will be made within a reasonable time and in a form that is readily comprehensible to the individual.

Subject to the CFC's lawful discretion, the existence, content, and source of information will not be made available to an individual unless required under G.L. c. 66, §10, the Massachusetts Public Records law or other law, when:

- disclosure would interfere with, compromise, or delay an on-going investigation or prosecution;
- disclosure would endanger the health or safety of an individual, organization, or community;
- the information is in an intelligence information system;
- The information is classified or otherwise not subject to disclosure under federal or state law.
- The CFC does not have the right to disclose the information.

Information gathered or collected and records retained by the CFC will not be:

- published, exchanged, or disclosed for commercial purposes;
- Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
- Disseminated to persons not authorized to access or use the information.

If an individual has a complaint or objection to the accuracy or completeness of information retained about him or her, originating with the agency, the CFC privacy officer will inform the individual of the procedure for requesting review of any objections. The individual will be given reasons if a request for correction of information that has been disclosed to the individual is denied. The individual will also be informed of the procedure for appeal when the agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates. A record will be kept of all requests for corrections and resulting action, if any.

If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that: (a) is exempt from disclosure, (b) has

been or may be shared through the ISE, (c) is held by the CFC, and (d) allegedly has resulted in demonstrable harm to the complainant, the center will inform the individual of the procedure for submitting (if needed) and resolving such complaints.

Complaints will be received by the CFC's Privacy Officer at Office of the Chief Legal Counsel, Massachusetts State Police General Headquarters, 470 Worcester Rd., Framingham, MA 01702, ATTN: CFC Privacy Officer and will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. All information held by the center which is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date.

If the information did not originate with the CFC, the MSP Commanding Officer or designee will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate.

To delineate protected information shared through the ISE from other data, the CFC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

INFORMATION RETENTION AND DESTRUCTION

Information within the criminal intelligence database will be reviewed for record retention in accordance with 28 CFR Part 23 (at least every five (5) years) and/or as specified by applicable state law pertaining to records retention.

The agency will remove information when the information has no further value or meets applicable criteria for removal according to CFC destruction policy and/or according to applicable State Records Retention Schedules.

The CFC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

Permission to destroy or return information or records will be presumed if in accordance with applicable State Retention Schedule(s) and subject to review by the CFC Privacy Officer.

Notification of proposed destruction or return of records may or may not be provided to the originating agency by the

CFC, depending on the relevance of the information and any agreement with the originating agency.

A record that information has been purged or returned shall be maintained by the CFC and, for criminal intelligence information system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date. For other systems, no notice of pending purge will be provided to originating agencies.

SECURITY SAFEGUARDS

The CFC's Security Officer is designated by the MSP Commander and will be trained to serve as the center's Security Officer.

The CFC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

The CFC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

Queries made to the CFC's data applications will be logged into the data system identifying the user initiating the query.

The CFC will utilize audit trails to track all types of information accessed, requested, and disseminated.

To prevent public records disclosure, risk and vulnerability assessments will be stored separately from publicly available data.

The security officer has primary responsibility for ensuring the systems that contain information are secure.

The CFC will follow the data breach notification guidance set forth in MGL c. 93H, §1 *et seq.* (Security Breach/Personal Information).

To the extent required by MGL c. 93H, §1 *et seq.*, CFC will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

ACCOUNTABILITY AND ENFORCEMENT

The CFC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be made available upon request, and posted on the Massachusetts State Police Web page at www.mass.gov/msp.
The CFC Privacy Officer, in consultation with the MSP Commander, will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the CFC's information

system. The Privacy Officer can be contacted at Office of the Chief Legal Counsel, Massachusetts State Police General Headquarters, 470 Worcester Rd., Framingham, MA 01702, ATTN: CFC Privacy Officer.

The MSP Commander is charged with overseeing the CFC operations and has the primary responsibility for the operation of this justice information system, including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy.

The CFC will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with National Criminal Intelligence Sharing Plan, the CFC Guidelines, Global's Applying Security Practices to Justice Information Sharing document, and 28 CFR Part 23.

The CFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer of the center.

The CFC will provide an electronic copy of this policy to all CFC and non-CFC personnel who are assigned to the CFC and will require written acknowledgment of receipt of this policy and agreement to comply with applicable provisions.

The CFC will annually conduct audits and inspections of the information contained in the CFC's Criminal Intelligence Database. The audits will be conducted randomly by a designated representative of the agency. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the CFC's information.

The CFC Privacy Oversight Committee will annually review this policy and recommend changes to the MSP Commander in response to changes in law and implementation experience.

The CFC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the CFC Privacy Officer.

The audit log of queries made to the CFC will identify the user initiating the query.

If an authorized user is found not to be in compliance with the provisions of this policy regarding the collection,

use, retention, destruction, sharing, classification, or disclosure of information, the CFC may, depending on the circumstances, do the following:

- suspend or discontinue access to information by the user;
- suspend, demote, transfer, or terminate the person(s) as permitted by applicable personnel policies and/or collective bargaining agreements;
- apply other sanctions or administrative actions as provided in agency personnel policies and/or collective bargaining agreements;
- request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or,
- refer, if appropriate, the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

The CFC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the center's privacy policy.

The CFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of two years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

TRAINING

The CFC will require, to the maximum extent feasible, the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties polices.

- CFC assigned personnel.
- Personnel providing information technology services to the agency.
- Staff in other public agencies or private contractors providing services to the CFC.
- Users who are not employed by the CFC or a contractor.
- The MSP Commander reserves the right to require any CFC employee or user to submit to appropriate training.

The CFC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

The training program will include instruction on:

- Purposes of the privacy, civil rights, and civil liberties protection policy.
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency.
- Originating and participating agency responsibilities and obligations under applicable law and policy.
- The impact of improper activities associated with information accessible within or through the agency.
- Mechanisms for reporting violations of center privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.
- Originating and participating agency responsibilities and obligations under applicable law and policy.

APPENDIX A
(Primary Terms & Definitions)

28 CFR Part 23 - Section 28 Part 23 of the Code of Federal Regulations. This code governs Criminal Intelligence Offices which receive federal funding to operate.

Access - Refers to the business rules, means, and processes by and through which agency participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another agency participant.

Agency - Agency refers to the (name of agency) and all agencies that access, contribute, and share information in the (name of agency)'s justice information system.

Analysis - The function of handling, sorting, and filing information, including the sifting out of useless information, the orderly arrangement of collected materials so relationships can be established, and the creation of a system for rapid retrieval of filed information.

Assessment - An estimate, evaluation, or appraisal of information content and its possible impact.

Audit Trail - In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication – The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords.

Authorization - The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication.

Authorized User - A person that is granted direct access to RIFC information whose position and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

Civil Liberties - Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights - The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments, and by acts of Congress.

Classification - A rating given stored information. A classification indicates access and dissemination restrictions.

Collation - Assembling in proper order to clarify or give meaning to information

Confidentiality - Confidentiality is closely related to privacy, but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out

of respect for, and to protect and preserve, the privacy of others. (See Privacy.)

Credentials – Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information or Data - Information deemed relevant to the identification of, and the criminal activity engaged in, by an individual or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information.

Data - Insert symbols, signs, descriptions, or measures.

Data Breach – The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media–including computer tapes, hard drives, or laptop computers containing such media–upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques

Data Protection - Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure - The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner - electronic, verbal, or in writing - to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination - The transmission of intelligence orally, in writing, electronically, or by any other means, from the person having custody of the intelligence to another person.

Electronically Maintained - Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted - Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail

Homeland Security Information–As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or

investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Information - Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Collection - Information for submission to the RIFC can be collected from a variety of sources, including, but not limited to: informants, print and electronic media, public records, subpoenaed documents, and undercover operations. Collection will always be based upon reasonable suspicion of criminal activity, and will be conducted by lawful methods

Information Quality - Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence - Information that has been processed (i.e., collected, evaluated, collated, analyzed, and reported).

Law - As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information - Law enforcement information means any information obtained by, or of interest to, a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation, or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of, or response to, criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Logs - Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. ***(See also Audit Trail.)***

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's

official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Originating Agency – The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

Personal Information - Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism.

Personally Identifiable Information—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:
Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number).
Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records). Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons - Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents

Privacy - Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy - A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection - This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information - Protected information is personal information or data about individuals that is subject to information privacy or other legal protections under the U. S. Constitution, laws, and regulations of the United States, such as civil rights laws and 28 CFR Part 23; and applicable Massachusetts constitution, and State of Massachusetts, local, and tribal laws, ordinances, and codes.

Public:

Public includes:

Any person and any for-profit or nonprofit entity, organization, or association; Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information; Media organizations; and Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

Employees of the agency; people or entities, private or governmental, who assist the agency/center in the operation of the justice information system; and Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Public Access - Public access relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Record - Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress - Internal procedures to address complaints from persons regarding protected information about them that is under the agency's/center's control.

Retention - ***(Refer to Storage)***

Right to Know – Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity

Security - Security refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely

availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Agency—Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

Storage [or Retention]: Refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Suspicious Activity – Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR) – Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information – Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-related Information - In accordance with Intelligence Reform and Terrorism Prevention Act, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the Information Sharing Environment facilitates the sharing of terrorism, including weapons of mass destruction information, and homeland security information, as defined in IRTPA Section 1016(a) (5) and the Homeland Security Act 892(f) (1) (6 U.S.C. § 482(f) (1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the Information Sharing Environment will facilitate the sharing of "terrorism information", as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not

include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

User – An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

Official: